

**Remarks**

Upon entry of the present amendment, Claims 1-31 will remain pending in the present application.

In the Amendment after Final Rejection dated March 28, 2006, claims 1, 9 and 10 were amended, and new claims 28-31 were added. The amendments were not entered per Advisory Action dated 4/12/2006 for failing to cancel finally rejected claims. Accordingly, the Applicant attempted to amend claims 1, 9 and 10, and add new claims 28-31, in the First Preliminary Amendment dated July 28, 2006. However, as pointed out by the Examiner in the Office Action dated 9/12/2006, the claim identifiers in the amendment were incorrect. The Applicant thanks the Examiner for pointing out the irregularities and herein amends claims 1, 10, 15 and 21, cancels claims 9 and 13, and adds new claims 28-31 using proper identifiers.

Applicant respectfully submits that the amendments to the claims are fully supported by the original disclosure, and introduce no new matter therewith. Based on the foregoing amendment and the following remarks, it is respectfully submitted that the instant application is in condition for allowance. Prompt reconsideration and withdrawal of the rejections is respectfully requested.

***Rejection under 35 U.S.C. § 103(s) based on Schneier, Ober, Arnold and Fischer***

Claims 1-9, 15-18, 28 and 29 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bruce Schneier, *Applied Cryptography, Second Edition*, p. 176-177 (“Schneier”), in view of U.S. Patent No. 6,307,936 to Ober et al. (“Ober”), further in view of U.S. Patent No. 6,175,924 to Arnold (“Arnold”), and in further view of U.S. Patent No. 6,141,423 to Fischer (“Fischer”). These rejections are respectfully traversed.

To establish a *prima facie* case for obviousness under 35 U.S.C. § 103(a), three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, ***the prior art reference (or references when combined) must teach or suggest all the claim limitations***. See M.P.E.P. § 2143 (emphasis added). It is submitted that the combination of the above-mentioned references fails to establish a *prima facie* case for obviousness because the combination does not teach each and every element of the claimed invention.

The present application on pages 2-4 discloses the issues arising in the conventional use of root keys for encrypting/decrypting encryption keys after the root key has been compromised. In the past, when a root key was compromised, the user had to request the key provider to physically attend the computer site and install replacement root keys. In contrast, embodiments of the present invention provide a method and a system that allows the key provider to securely transfer the root key to the user via an information network such as the Internet. As such, the user can request a new root key and the request can be handled instantaneously by the key provider without jeopardizing the security of the root key.

Accordingly, claim 1 recites a method of transferring a root key between a key provider system and a second system via an information network. The method comprises a ***first super-root key*** in the key provider system; a ***second super-root key*** provided within the read-only memory circuit of the user's system (i.e. the second other system); and a ***first root key*** that is encrypted using the first super-root key of the key provider system, transferred to the user's system, and decrypted using the second super-root key; wherein the first root key is usable for encrypting and/or

decrypting *private keys*. It is respectfully submitted that neither of the references cited in the Action, nor the combination, teach encrypting a root key using a first super-root key of the key provider system and decrypting the root key at the user's system (i.e. the second other system) using a second super-root key.

Section 8.3 of Schenier whimsically describes Alice's problems in transferring securely a key she generated to Bob. Schenier describes methods that Alice can use to transfer the key to Bob (i.e. meeting Bob in a back alley, using alternate secure channels, a trusted messenger, splitting the key into several different parts and sending each part over a different channel, etc.). Each method described by Schenier, however, constitutes nothing more than creating a communication channel. Schenier also discloses the X9.17 standard which uses key-encryption keys and data keys, wherein key-encryption keys are used to encrypt data keys for distribution. However, Schenier does not disclose using a super-root key to encrypt or decrypt the key-encryption keys. Schenier teaches nothing more than what the present application describes in pages 2-4 as security issues in the related art. In fact, Schenier teaches away from using a super-root key because on the last paragraph of page 176 of Schenier, where it states that the "key-encryption keys have to be distributed manually."

The Action argues that Ober supplements the deficiencies of Schenier described above. On page 4, second full paragraph, the Action argues that Ober teaches the three different levels of keys, i.e. super root key, root key and private key, where the LSV is the super root key, the GKEK is the root key and the remaining keys are the private keys. It is respectfully submitted that neither Ober nor its combination with Schenier teaches or suggests using a first super-root key of the key provider system to encrypt a root key, transmitting the encrypted root key to a second other system,

and using a second super-root key in the second other system to decrypt the root key. Ober merely discloses a method and process of managing encryption keys in a cryptographic co-processor, which includes selecting a key type (symmetrical or asymmetrical), selecting the bit length of the key, generating key, and finally presenting the key in internal or external form. *See FIG. 1.*

The Action's claim that the LSV is the super root key, the GKEK is the root key, and the remaining keys are private keys, is misplaced. Ober discloses data encryption keys (DEKs) and key encryptions keys (KEKs) as two types of symmetric keys. *See Col. 2: 61 – Col. 3: 16.* KEKs include GKEK (an internally generated storage variable), LSV (a local storage variable), and application KEKs. The LSV is a non-volatile KEK which is laser-burned into each CypticIC device at fabrication and is considered the chip's master root key. *See Col. 10: 31-35.* The GKEK are internally generated KEKs that allow the application to safely build its own symmetric key hierarchy tree securely. *See Col. 10: 38-42.* The sole purpose of the GKEK is to limit the exposure of the LSV to effectively insulate the LSV from direct attacks. *See Col. 24: 37-46.* The application creates trusted KEKs, which cover other untrusted KEKs as well as DEKs, directly under the GKEK. *See FIG. 2 and Col. 24: 38-52.* This structure is substantially different from the system of the present application comprising a first super-root key, a second super-root key, and a root key used to encrypt/decrypt private keys.

The LSV of Ober does not teach or suggest the second super key of the present application. The LSV is laser-burnt into the CypticIC device at fabrication, whereas the second super-root key within the second other system is stored in a read-only memory of a first secure module. In fact, the CypticIC system of Ober does not even include non-volatile memory. *See Col. 23: 64.* The second super-root key, however, can be manually replaced by the key-provider system. Also, the

second super-root key of the present application is used only in rare instances when a new root key is requested by the use and the key provider system transfers an encrypted root key to the user's system. The LSV of Ober, on the other hand, is used whenever a KEK within the tree is needed to encrypt/decrypt a DEK.

The GKEK and KEKs of Ober also fail to teach or suggest the root key of the present application. The root key of the present application is transferable from the key provider system to the second other system and is decrypted using the second super-root key. The GKEK, however, is not exportable and is used only to provide an additional protection between the KEKs and the LSV. As shown in FIG. 2 of Ober, the KEKs (i.e. the trusted uKEK that covers the untrusted DEK) are also non-exportable. Therefore, the GKEK and KEKs of Ober not only fail to teach or suggest the root key of the present invention, they teach away from this feature of the present invention.

Even assuming for purposes of argument that the LSV is equivalent to a super root key, Ober does not disclose encrypting a root key using a first LSV in a first system, transferring the root key into a second system, and decrypting the root key using a second LSV within the second system.

For at least the reasons stated above, the combination of Ober and Schenier fails to teach or disclose using a first super-root key of the key provider system to encrypt a root key, transmitting the encrypted root key to a second other system, and using a second super-root key in the second other system to decrypt the root key. Arnold and Fischer also fail to supplement the deficiencies of the combination of Ober and Schenier. Specifically, Arnold only discloses two types of keys: the private key  $K_{PR}$  and the public key  $K_{PU}$ , and thus does not teach a relationship between a data key, a root key, and a super-root key, including encrypting the root key using a first super-root key and

later decrypting it using a second super-root key. *See Arnold, Col. 5: 31-38.* Fischer discloses a private key, a random DES key, a public key, and a trustee's public key, but none of the disclosed keys are used to encrypt/decrypt a key encryption key (i.e. root key), nor does Fischer disclose transferring root keys between a key provider system and a second system. *Col. 4: 59-61, Col. 7: 28-33 and Col. 9: 58-60.* Since Schenier, Ober, Fischer and Arnold, either alone or in combination, do not teach each and every element of claim 1, a *prima facie* case for obviousness under 35 U.S.C. 103(a) has not been established.

Furthermore, even if the combination of the references disclosed every element of claim 1, there is no motivation or suggestion in the prior art references make the proposed combination. In fact, as previously discussed, Schenier teaches away from the proposed combination because it states that the "key-encryption keys have to be distributed manually," thereby teaching away from using a super-root key to encrypt/decrypt the key-encryption keys and transferring the key-encryption keys from one system to another. Also, Ober teaches away from using a memory to store the LSV in order to increase security of the LSV and instead discloses laser-burning the LSV into the CypticIC device at fabrication. Therefore, it is respectfully submitted that at the time of the invention, the cited references could not have been combined by a person of ordinary skill in the art to teach each and every element of the present invention. Accordingly, the Action has not established a *prima facie* case for obviousness under 35 U.S.C. 103(a).

For at least these reasons, it is submitted that claim 1 is patentably distinguishable over the prior art. Claims 2-9 and 28 are directly or indirectly dependent claim 1 and should be allowed for at least the same reasons. Withdrawal of the rejections and reconsideration of claims 1-9 and 28 is respectfully requested.

Claim 15 recites "a system for transferring a secure root key between a key provider system and a second other system ... comprising a secure module in operative communication with the second other system." The secure module comprises a memory storage unit having program code for decrypting an encrypted secure root key using the first super-root key. For at least the reasons previously stated for claim 1, Schenier, Ober, Fischer and Arnold, either alone or in combination, fail to teach each and every element of claim 15. Therefore, as in claim 1, a *prima facie* case for obviousness under 35 U.S.C. § 103(a) has not been established. Accordingly, it is submitted that claim 15 is patentably distinguishable over the prior art. Claims 16-18 and 30 are directly or indirectly dependent claim 15 and should be allowed for at least the same reasons discussed above. Withdrawal of the rejections and reconsideration of claims 15-18 and 30 is respectfully requested.

***Rejection under 35 U.S.C. § 103(s) based on Schenier, Ober, Arnold, Fischer and Spelman***

Claims 10-14 and 29 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Schenier, Ober, Arnold and Fischer, and in further view of Patent No. 5,680,458 to Spelman et. al ("Spelman"). These rejections are respectfully traversed. Specifically, claim 10 recites some of the same features as claim 1 including "encrypting the *first root key* using a *first super-root key* of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the *first root key* is useable for at least one of encrypting and decrypting *private keys*." Therefore, for at least the same reasons previously discussed, claim 10 is patentably distinguishable over Schenier, Ober, Arnold and Fischer, individually or in combination. Spelman fails to cure the deficiencies of Schenier, Ober, Arnold and Fischer previously discussed. Accordingly, it is respectfully submitted that claim 10 is patentably distinguishable over the prior art and should be allowed. Claims 11-14 and 29 are

dependent on claim 10 and should be allowed for at least the same reasons. Withdrawal of the rejections and reconsideration of claims 10-14 and 29 is respectfully requested.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Easter***

Claim 19 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schenier, Ober, Arnold and Fischer and in further view of U.S. Patent No. 5,598,889 to Easter ("Easter"). Applicant respectfully traverses this rejection. Specifically, claim 19 is indirectly dependent on claim 15. Therefore, for at least the same reasons previously discussed for claim 15, claim 19 is patentably distinguishable over Schenier, Ober, Arnold and Fischer, individually or in combination. Easter fails to cure the deficiencies of Schenier, Ober, Arnold and Fischer previously discussed. Accordingly, it is respectfully submitted that claim 19 is patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claim 19 is respectfully requested.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Bergum***

Claim 20 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schenier, Ober, Arnold and Fischer and in further view of U.S. Patent No. 5,249,277 to Bergum et. al ("Bergum"). Applicant respectfully traverses this rejection. Specifically, claim 20 is indirectly dependent on claim 15. Therefore, for at least the same reasons previously discussed for claim 15, claim 20 is patentably distinguishable over Schenier, Ober, Arnold and Fischer, individually or in combination. Bergum fails to cure the deficiencies of Schenier, Ober, Arnold and Fischer previously discussed. Accordingly, it is respectfully submitted that claim 20 is patentably



distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claim 20 is respectfully requested.

***Rejection under 35 U.S.C. § 103(a) based on Schenier, Ober, Arnold, Fischer, Spelman, Mason and Ehram***

Claims 21-24 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schenier, Ober, Arnold, Fischer and Spelman and in further view of U.S. Patent No. 6,331,784 to Mason et. al (“Mason”). Applicant respectfully traverses this rejection. Specifically, claim 21 recites features similar to claim 10 including encrypting the ***first root key*** using a ***third super-root key*** of the key provider, transferring the encrypted first root key from the key provider system to the second other system via the information network, and the ***first root key*** being useable for at least one of encrypting and decrypting ***private keys***. Therefore, for at least the same reasons previously discussed for claim 10, claim 21 is patentably distinguishable over Schenier, Ober, Arnold, Fischer and Spelman, individually or in combination. Mason fails to cure the deficiencies of Schenier, Ober, Arnold, Fischer and Spelman previously discussed. Accordingly, it is respectfully submitted that claim 21 is patentably distinguishable over the prior art and should be allowed. Claims 22, 23 and 31 are dependent on claim 21 and should be allowed for at least the same reasons. Withdrawal of the rejections and reconsideration of claim 21-23 and 31 is respectfully requested.

Claim 25 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schenier, Ober, Arnold, Fischer, Spelman and Mason and in further view of U.S. Patent No. 4,386,234 to Ehram et. al (“Ehram”). Applicant respectfully traverses this rejection.

Specifically, claim 25 is indirectly dependent on claim 21. Therefore, for at least the same reasons previously discussed for claim 21, claim 25 is patentably distinguishable over Schenier, Ober, Arnold, Fischer, Spelman and Mason, individually or in combination. Ehram fails to cure the deficiencies of Schenier, Ober, Arnold, Fischer, Spelman and Mason previously discussed. Accordingly, it is respectfully submitted that claim 25 is patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claim 25 is respectfully requested.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Spelman, Mason, Ehram and Easter***

Claim 26 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schenier, Ober, Arnold, Fischer, Spelman, Mason and Ehram and in further view of U.S. Patent No. 5,598,889 to Easter et. al ("Easter"). Applicant respectfully traverses this rejection. Specifically, claim 26 is dependent on claim 25. Therefore, for at least the same reasons previously discussed above, claim 26 is patentably distinguishable over Schenier, Ober, Arnold, Fischer, Spelman, Mason and Ehram, individually or in combination. Easter fails to cure the deficiencies of Schenier, Ober, Arnold, Fischer, Spelman, Mason and Ehram previously discussed. Accordingly, it is respectfully submitted that claim 26 is patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claim 26 is respectfully requested.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Spelman, Mason, Ehram, Easter and Bergum***

Claim 27 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schenier, Ober, Arnold, Fischer, Spelman, Mason, Ehram and Easter and in further view of Bergum. Applicant respectfully traverses this rejection. Specifically, claim 27 is dependent on claim 26. Therefore, for at least the same reasons previously discussed above, claim 27 is patentably distinguishable over Schenier, Ober, Arnold, Fischer, Spelman, Mason, Ehram and Easter, individually or in combination. Bergum fails to cure the deficiencies of Schenier, Ober, Arnold, Fischer, Spelman, Mason, Ehram and Easter previously discussed. Accordingly, it is respectfully submitted that claim 27 is patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claim 27 is respectfully requested.

***Conclusion***


All of the stated grounds of rejection have been properly traversed. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

No additional fees are believed to be required. However, if the Office deems that any fees are necessary, authorization is hereby granted to charge any required fees to Deposit Account No. 22-0261.

In view of the above amendment, applicant believes the pending application is in condition for allowance. Prompt and favorable consideration of this Amendment is respectfully requested.

Dated: December 12, 2006

Respectfully submitted,

By   
Jeffri A. Kaminski  
Registration No.: 42,709  
James R. Burdett  
Registration No.: 31,594  
VENABLE LLP  
P.O. Box 34385  
Washington, DC 20043-9998  
(202) 344-4000  
(202) 344-8300 (Fax)  
Attorney/Agent For Applicant

*REG NO 31,594*